AFFIDAVIT

I, Terrance L. Taylor, being duly sworn, do hereby depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the seizure and examination of property— two (2) electronic devices as further described in Attachment A—which are currently in the possession of the Department of Homeland Security, Homeland Security Investigations, 210 Kanawha Boulevard West, Charleston, Kanawha County, West Virginia 25302, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been so employed since March 2012. I am currently assigned to the Office of the Resident Agent in Charge HSI Charleston, West Virginia. I have experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

3. I am a Special Agent with twenty-one years of federal law enforcement experience. Prior to my employment with HSI, I was a Police Officer for two years in Huntington, West Virginia, a Special Agent with the United States Department of State-Bureau of Diplomatic Security for six years, a Special Agent with the Naval Criminal Investigative Service for two years, and a Special Agent with the United States Department of State-Office of

Inspector General for two years. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Center ("FLETC") and a graduate of the West Virginia State Police Academy. I graduated from the Criminal Investigator Training Program in 2002, and the Immigration and Customs Enforcement Special Agent Training Program in 2012. As part of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. These areas include laws and regulations pertaining to the importation of various types of merchandise and contraband, prohibited items, money laundering, and various immigration violations. I have more specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to 18 U.S.C. §§ 2251, 2252, 2252A, and 2256.

4. As a Special Agent, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the FLETC, Immigration and Customs Enforcement, as well as everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child pornography that occur in the District of Southern West Virginia. I have received training in the areas of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8)) in all forms of media, including computer media. I have obtained search warrants for child pornography offenses, and I have been the case agent or assisted others in numerous investigations involving the sexual exploitation of children. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography) and

2252A(a)(5)(B) (possession of child pornography), and I am authorized by law to request a search warrant.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The probable cause statement is based upon information of which I am personally aware as well as information that has been conveyed to me by other law enforcement officers.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. The property to be searched consists of two (2) electronic devices, which are described in more detail in Attachment A (the "Devices"). The Devices are presently located at the Department of Homeland Security, Homeland Security Investigations, 210 Kanawha Boulevard West, Charleston, Kanawha County, West Virginia 25302. The Devices were voluntarily provided to law enforcement by the owner and current resident of the home where Jason Doliver MCSWEENEY ("MCSWEENEY") lived prior to his arrest and incarceration on September 24, 2023. Prior to his arrest, MCSWEENEY lived with the owner of the residence (his mother, whose identity is known to investigators but who shall be referred to herein as "D.M."), and she had access to the entirety of the residence, including the places where the Devices were located. Upon information and belief, the Devices are in the same condition as they were when MCSWEENEY was arrested and incarcerated on September 24, 2023.

7. The applied-for warrant would authorize the seizure and forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

STATUTES UNDER INVESTIGATION

8. I am currently investigating MCSWEENEY for violations of 18 U.S.C.

§ 2252A(a)(1) and (2) (transportation, receipt, and/or distribution of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography). I seek to search the Devices to locate evidence of criminal violations set forth above for items specified in Attachment B, incorporated herein by reference.

BACKGROUND ON PEER-TO-PEER (P2P) FILE SHARING

9. Based on my training and experience, I know the following regarding peer-to-peer file sharing networks, peer-to-peer client software programs, and the BitTorrent peer-to-peer file sharing network. A growing phenomenon on the Internet is peer-to-peer (hereinafter referred to as "P2P") file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software programs. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the Internet. There are multiple types of P2P file sharing networks on the Internet. To connect to a particular P2P file sharing network, a user first obtains a P2P client software program for a particular P2P file sharing network, which can be downloaded from the Internet. A particular P2P file sharing network may have many different P2P client software programs that allow access to that particular P2P file sharing network. Additionally, a particular P2P client software program may be able to access multiple P2P file sharing networks.

10. These P2P client software programs share common protocols for network access and file sharing. The user interface, features, and configurations may vary between clients and versions of the same client. In general, P2P client software allows the user to set up file(s) on a computer to be shared on a P2P file sharing network with other users running compatible P2P client software. A user can also obtain files by opening the P2P client software on the user's

computer and conducting a search for files that are of interest and currently being shared on a P2P file sharing network. Some P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files.

11. Settings within these programs control sharing thresholds. Typically, during a default installation of a P2P client software program, settings are established which configure the host computer to share files. Depending upon the P2P client software used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed. A setting establishes the location of one or more directories or folders whose contents (digital files) are made available for distribution to other P2P clients. In some clients, individual files can also be shared. A setting controls whether or not files are made available for distribution to other P2P client and whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. The latter feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.

12. Typically, files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value is computed for each file and/or piece of a file being shared (dependent on the P2P file sharing network), which uniquely identifies it on the network. A file (or piece of a file) processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this,

users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process. P2P file sharing networks, including the BitTorrent network, are frequently used to trade digital files of child pornography. These files include both image and movie files.

13. The BitTorrent network is a very popular and publicly available P2P file sharing network. Most computers that are part of this network are referred to as "peers." The terms "peers" and "clients" can be used interchangeably when referring to the BitTorrent. A peer can simultaneously provide files to some peers while downloading files from other peers. The BitTorrent network can be accessed by computers running many different client programs, some of which include the BitTorrent client program, uTorrent client program, and Vuze client program. These client programs are publicly available and free P2P client software programs that can be downloaded from the Internet. There are also BitTorrent client programs that are not free. These BitTorrent client programs share common protocols for network access and file sharing. The user interface, features, and configuration may vary between clients and versions of the same client. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files. Depending upon the BitTorrent client used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed.

14. A setting establishes the location of one or more directories or folders whose contents (files) are made available to other BitTorrent network users to download.

In order to share a file or a set of files on the BitTorrent network, a "Torrent" file needs to be created by the user that initially wants to share the file or set of files. A "Torrent" is typically a small file that describes the file(s) that are being shared, which may include information on how to locate the file(s) on the BitTorrent network. A typical BitTorrent client will have the ability to create a "Torrent" file. It is important to note that the "Torrent" file does not contain the actual file(s) being shared, but information about the file(s) described in the "Torrent," such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent."

15. The "info hash" of each "Torrent" uniquely identifies the "Torrent" file. The "info hash" is a SHA-1 hash value of the set of data describing the file(s) referenced in the "Torrent," which include the SHA-1 hash value of each file piece, the file size, and the file name(s). SHA-1, or Secure Hash Algorithm Version 1, is a file encryption method which may be used to produce a unique digital signature of a file. Finding a file that produces the same SHA-1 value as a known file requires a search and comparison of 1048 (2160) different files, which is computationally infeasible. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard.

16. The "Torrent" file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers." "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the

"Torrent." It is important to note that the "Trackers" do not actually have the file(s) and are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network is not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

17. Once a "Torrent" is created, in order to share the file(s) referenced in the "Torrent" file, a user typically makes the "Torrent" available to other users, such as via websites on the Internet. In order to locate "Torrent" files of interest, a typical user will use keyword searches within the BitTorrent network client itself or on websites hosting "Torrents." Once a "Torrent" file is located that meets the keyword search criteria, the user will download the "Torrent" file to their computer. Alternatively, a user can also search for and locate "magnet links," which are links that enable the BitTorrent network client program itself to download the "Torrent" to the computer. In either case, a "Torrent" file is downloaded to the user's computer. The BitTorrent network client will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file. It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent," to include the remote peers'/clients' Internet Protocol (IP) addresses.

18. Two computers on the Internet identify each other by an IP address. IP addresses can assist law enforcement in finding a particular computer on the Internet and thereby lead law enforcement to a person of interest. A person interested in obtaining child pornographic images on the BitTorrent network would open the BitTorrent client application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." (It should be noted that this particular situation did not occur in this investigation.) The results of the keyword search are typically returned to the user's computer by displaying them on the "Torrent" hosting website. The hosting website will typically display information about the "Torrent," which can include the name of the "Torrent" file, the name of the file(s) referenced in the "Torrent" file, the size of the file(s), and the "info hash" SHA-1 value of the "Torrent" file. The user then selects a "Torrent" of interest to download to their computer. Typically, the BitTorrent client program will then process the "Torrent" file. The user selects from the results displayed the file(s) they want to download that were referenced in the "Torrent" file. Utilizing trackers and other BitTorrent network protocols (such as Distributed Hash Tables, Peer Exchange, and Local Peer Discovery), peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file(s) is then downloaded directly from the computer(s) sharing the file. Typically, once the BitTorrent network client has downloaded part of a file(s), it may immediately begin sharing the file with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 piece hash described in the "Torrent" file. During the download process, a typical BitTorrent client program displays the IP address of the peers/clients that appear to be sharing part or all of the file(s) referenced in the "Torrent" file or other methods utilized by the BitTorrent network protocols. The downloaded

file is then stored in the area previously designated by the user and/or the client program. The downloaded file(s), including the "Torrent" file, will remain until moved or deleted.

19. As described above, one method for an investigator to search the BitTorrent network for users possessing and/or disseminating child pornography files is to type in search terms that, based on the investigator's training and experience, would return a "Torrent" filename indicative of child pornography. The investigator would then download the file(s) referenced within the "Torrent" file and determine if the file(s) indeed contained child pornography. The investigator can document the "info hash" SHA-1 hash value of this "Torrent" file, to be compared with future identical "Torrent" files observed on the BitTorrent network. Although transparent to the typical user, when searches are conducted, additional results are received from the "Trackers" on other peers who recently reported to the network as having that file(s) in whole or in part, which may include the IP addresses of those peers/clients. This information can be documented by investigators and compared to those "info hash" SHA-1 hash values the investigator has obtained in the past and believes to be child pornography, which allows for the detection and investigation of computers involved in possessing, receiving, and/or distributing files of previously identified child pornography. Therefore, without even downloading the file(s), the investigator can compare the "info hash" SHA-1 hash value and determine with mathematical certainty that a file(s) seen on the network is an identical copy of a child pornography file(s) they had seen before.

20. The returned list of IP addresses can include computers that are likely to be within the investigator's jurisdiction. The ability to identify the approximate location of these IP addresses is provided by IP geographic mapping services, which are publicly available and also used for marketing and fraud detection. At this point in the investigative process, an association

between a known "Torrent" file (based upon on the "info hash" SHA-1 hash value comparison) and a computer having a specific IP address (likely to be located within a specific region) can be established. Once a client user is identified as recently having a file(s) believed to be child pornography, in whole or in part, the investigator can then query that client user directly to confirm the client user has that file(s), in whole or in part, and/or download that file directly from the client user exclusively, otherwise known as a single source download. Depending upon several factors, including configuration and available resources, it might not be possible to do either.

21. The process of sharing files on the BitTorrent network involves peers allowing other peers to copy a file(s) or portions of a file(s). This sharing process does not remove the file(s) from the computer sharing the file. This process places a copy of the file on the computer which downloaded it. If an investigator either received an affirmative response from a remote peer that they possess a digital file, or the investigator received a digital file, in whole or in part, that is believed to contain child pornography, from a remote peer at a specific IP address, the investigator can conclude that a computer, likely to be in this jurisdiction, is running a BitTorrent network P2P client and is currently possessing, receiving, and/or distributing specific and known visual depictions of child pornography. Law enforcement has created BitTorrent network client programs that obtain information from "Trackers" about peers/clients recently reporting that they are involved in sharing digital files of known actual child pornography (based on the "info hash" SHA-1 hash value), which then allows the downloading of a file from a single IP address (as opposed to obtaining the file from multiple peers/clients on the network). This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography on the BitTorrent network. During the query and/or downloading

process from a remote BitTorrent network client, certain information may be exchanged between the investigator's client and the remote client they are querying and/or downloading a file from, such as 1) the remote client's IP address; 2) a confirmation from the remote client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) are being reported as shared from the remote client program; and 3) the remote client program and version. This information may remain on the remote client's computer system for long periods of time. The investigator has the ability to log this information. A search can later be conducted on a seized computer system(s) for this information, which may provide further evidence that the investigator's client communicated with the remote client.

22. An analogy to this investigative methodology would be receiving information from an informant or an anonymous source that a particular residence was selling illegal narcotics. An undercover investigator could independently confirm this information by knocking on the door of the residence and asking if the occupants had said illegal narcotics. If so, the undercover investigator would then ask for and receive the said illegal narcotics without actually entering the residence, which would be similar to asking for and receiving an illegal child pornography file from a P2P peer/client. The investigation of peer-to-peer file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children Task Force Program. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of which were also involved in the sexual exploitation of actual child victims.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, WIRELESS TELEPHONES, THE INTERNET, AND EMAIL

23. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

24. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). Darkroom facilities and a significant amount of skills were required in order to develop and reproduce the photographic images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their detection by the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

25. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

26. Child pornographers can now transfer photographs from a camera in a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer or wireless telephone. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it

inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through File Transfer Protocols to anyone with access to a computer or wireless telephone capable of Internet access. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, computers and wireless telephones are preferred methods of distribution and receipt of child pornographic materials among pornographers.

27. A computer or wireless telephone's ability to store images in digital form makes them ideal repositories for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers and other electronic devices such as cell phones or even gaming consoles has increased tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

28. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

29. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Inc., and Google, Inc., among others. The online services allow a user to set up an account with remote access. Even in cases where online storage is used, however, evidence of child pornography can often be found on the user's computer or wireless telephone.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

30. Based upon my knowledge, experience, and training in criminal investigations, particularly those that focus on child exploitation, as well as the training and experience of other law enforcement officers trained in child exploitation and child pornography investigations with whom I have had discussions, there are certain characteristics common to individuals involved in the possession, receipt and distribution of child pornography:

a) Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b) Collectors of child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce or to arouse the selected child partner, or to demonstrate the desired sexual acts.

c) Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d) Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e) Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended

periods of time even after the individual "deleted" it.[1]

f) Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g) Collectors of child pornography prefer not to be without their child pornography for any prolonged time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. It has long been recognized by professionals dealing with persons involved with child pornography that child pornography has enduring value to those involved in the sexual exploitation of children. Such persons rarely, if ever, dispose of their sexually explicit material. Those materials are often treated as prized possessions. Individuals involved in child pornography almost always maintain their materials in a place that they consider secure and where the materials are readily accessible. Most frequently, these materials are kept within the privacy and security of their own homes. These materials are often kept on their person in forms of media storage devices such as thumb drives and cellphones in their pants pockets and on their keychains.

h) Further, it is common for such users to save and transfer the pornographic images and/or pornographic video of children from one computer to another because the images are generally difficult to obtain securely.

31. Your Affiant believes that given the continuing nature of possession of child pornography and the general character of such offenders as "collectors" and "hoarders," there is probable cause to believe that evidence of violations of federal law, including, but not limited to, 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography) and 2252A(a)(5)(B)

---

[1] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

(possession of child pornography) will be present on the Devices, as described in Attachment A, when the search is conducted.

DEFINITIONS

32. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

c. Computer: As defined in 18 U.S.C.§ 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

d. Child pornography: As defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable form, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

e. Sexually explicit conduct. As defined in 18 U.S.C. § 2256(2)(A)(i-v), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

f. Visual depiction. As defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means which is

capable of conversion into a visual image, and data which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

33. On or about January 11, 2023, at 21:05 hours through on or about January 13, 2023, at 13:57 hours, Parkersburg Police Department Detective Daniel Miller was running BitTorrent software and was connected to the Internet in an undercover capacity to conduct an investigation on the BitTorrent P2P file sharing network. A connection was made between the investigative computer and a computer/computing device running BitTorrent software having an IP address assigned as 73.152.138.46. Two files, one consisting of 78 pieces and the other of 387 pieces were successfully downloaded from IP address 73.152.138.46. The device at IP address 73.152.138.46 was the only IP address which shared the contents for each file downloaded, whether completed or not, and as such, each file was downloaded directly from this IP Address. Both of the files being shared that Detective Miller downloaded clearly constitute child pornography whether in part or in whole. The following files were viewed by Detective Miller:

a) **"mov_0216.mp4"** This video file depicts two prepubescent, female children laying on a green colored couch/bench. One child is laying on her back with the other child laying on her back on top of the other child. An adult male penis can be seen penetrating the vagina of the child on the bottom and then penetrating the vagina of the child on top.

b) **"(G)Paradise Birds Anna & Nelly BDSM p6_recode.avi"** This video file depicts two prepubescent, female children in a bedroom near a bed. One of the children takes her top and bottom off and lays on the bed while the other clothed child ties her wrists to the headboard with pieces of rope.

34. On or about January 30, 2023, Detective Miller filed and submitted an administrative subpoena requesting subscriber information from Comcast Cable Communications on the aforementioned timeframe when the child pornography files were downloaded by Detective Miller from IP address 73.152.138.46. Comcast Cable Communications subsequently responded to the administrative subpoena and indicated that the subscriber of the IP address was Paris Sweeney of 223 31st Street West, Huntington, West Virginia 25704.

35. On or about March 17, 2023, at 02:26 hours through on or about May 12, 2023, at 18:24 hours, Detective Miller was running BitTorrent software and was connected to the Internet in an undercover capacity to conduct an investigation on the BitTorrent P2P file sharing network. During that time multiple connections were made between the investigative computer and a computer/computing device running BitTorrent software having an IP address assigned as 76.26.77.74. Seven files were successfully downloaded in total or partially from IP address 76.26.77.74. The device at IP Address 76.26.77.74. was the only IP address which shared the contents for each file downloaded, whether completed or not, and as such, each file was downloaded directly from this IP Address. All the files being shared that Detective Miller downloaded clearly constitute child pornography whether in part or in whole. The following files were viewed by Detective Miller:

a) **"000098.avi"** This video file depicts a prepubescent, female child being vaginally penetrated by an adult male penis and a dildo.

b) **"000238.mp4"** This video file depicts a prepubescent, female child being vaginally penetrated by an adult male penis.

c) **"001066.wmv"** This video file shows a prepubescent unknown gender child being anally penetrated by an adult male penis.

d) **"001712.wmv"** This video file depicts a prepubescent, female child being vaginally penetrated by an adult male penis. The male ejaculates on the child's vagina.

e) **"001720.AVI"** This video file depicts a prepubescent, female child being vaginally penetrated by an adult male penis. The child has the words "FUCK ME" written on her stomach with an arrow pointing toward her vagina. The video changes to another prepubescent, female child digitally penetrating her own vagina while saying "fuck my pussy" to the camera.

f) **"!!! New 2006 !!! Guatemala 9Yo Nena De La Calle (Sopp2) {Rare Reel Fck Good} (Kleuterkutje) (Pedo) (Ptsc) Very Good (Pthc) 12Y American Indian Girl Fucked.avi"** This video file depicts a prepubescent, female child laying in the backseat of a vehicle while being vaginally penetrated by an adult male penis.

g) **"OPVA PTHC 2015 11yo and uncle best anal fuck creampie ever!!!!!.avi"** This video depicts a prepubescent, female child being anally penetrated by an adult male penis. The child can be heard crying as the adult male penis penetrates her and ejaculates in her anus.

36. On or about March 28, 2023, Detective Miller filed and submitted an administrative subpoena requesting subscriber information from Comcast Cable Communications on the aforementioned timeframe when the child pornography files were downloaded by Detective Miller from IP address 76.26.77.74. Comcast Cable Communications

subsequently responded to the administrative subpoena and indicated that the subscriber to the IP address was Paris Sweeney of 223 31st Street West, Huntington, West Virginia 25704.

37. On or about November 13, 2023, Detective Miller contacted your Affiant regarding the P2P investigation. Your Affiant conducted investigative checks on the 223 31st Street West, Huntington, West Virginia, residence. A search of the Wayne County, West Virginia, Assessor's Tax Map identified D.M. as the owner of the residence located at 223 31st Street West, Huntington, Wayne County, West Virginia.

38. West Virginia Department of Motor Vehicles records showed that D.M. was issued an identification card with identification number I421012 on September 16, 2021.The identification card listed D.M.'s address as 223 31st Street West, Huntington, Wayne County, West Virginia.

39. Further investigation revealed that MCSWEENEY also resided at 223 31st Street West, Huntington, Wayne County, West Virginia. West Virginia Department of Motor Vehicles records showed that MCSWEENEY was issued a driver's license with license number E751488 on August 28, 2018. The driver's license listed MCSWEENEY's address as 223 31st Street West, Huntington, Wayne County, West Virginia.

40. On or about November 16, 2023, your Affiant and HSI Special Agent Christopher Yarnell conducted a voluntary interview with D.M. at her residence located at 223 31st Street West, Huntington, Wayne County, West Virginia. Your Affiant advised D.M. that a child exploitation investigation was associated with her IP address at the residence. D.M. agreed to be interviewed regarding the investigation.

41. During the interview, D.M. stated the following: Her husband died a few years ago, and it has only been herself and her son, MCSWEENEY, residing in her house. She has

Comcast as her internet service provider, and her wi-fi router is password protected. No other people visit her residence, and no one else has the router password except for her son, MCSWEENEY. Her son has bi-polar disorder and is not currently on any medication. He does not work, nor does he collect Social Security disability benefits. Their income consists of her husband's pension and Social Security benefits. MCSWEENEY was recently arrested for a domestic violence offense and is incarcerated. D.M. is expected to testify in Wayne County court on December 6, 2023, regarding his arrest.

42. Regarding electronic devices within her home, D.M. stated the following: She has a desktop computer in her family room and a personal cellphone with the phone number is 304-XXX-XX05. D.M. is not aware of MCSWEENEY viewing child pornography, but acknowledges he does watch videos on the desktop computer and an Amazon tablet. However, she does not know what he watches because she is legally blind and would not be able to view any images on the computer. MCSWEENEY has one of D.M.'s old cellphones and one of her old Amazon tablets in his bedroom.

43. D.M. allowed your Affiant and SA Yarnell to view MCSWEENEY's room to find his electronic devices. Your Affiant asked D.M. if she would sign a Consent to Search form regarding the desktop computer, her old cellphone, and her old Amazon tablet. She subsequently agreed to allow HSI Charleston to conduct a computer forensic review of the aforementioned items by signing the document. Your Affiant provided D.M. an inventory of the three items to be taken for a computer forensic review.

44. On or about December 9, 2023, a computer forensic review was completed on the Asus desktop computer that was located in D.M.'s living room adjacent to the front door. The computer forensic review identified 5,431 images and 9 videos of child pornography.

45. Law enforcement did not conduct a computer forensic review of the Amazon tablet and D.M.'s old cellphone because those devices were located in MCSWEENEY's bedroom. This search warrant seeks a computer forensic review of those items.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER AND ELECTRONIC DEVICE SYSTEMS

46. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers and other electronic devices, I know that data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

47. As is the case with most digital technology, communications by way of computer or cellular phone can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used.

48. I submit that there is probable cause to believe the items in Attachment B will be stored on the Devices for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

49. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

d. Moreover, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

e. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

f. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

g. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

h. I know that when an individual uses a computer to distribute or attempt to distribute child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for

evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

FORENSIC ANALYSIS

50. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant. If the Devices have been locked using a passcode, the examination may also include the use of computer programs or other devices to bypass the passcode or otherwise access the material located on the Devices.

CONCLUSION

51. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

52. Moreover, I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, unless otherwise ordered by the Court, the return will not include the specific evidence later examined by a forensic analyst.

Further your Affiant sayeth naught.

SPECIAL AGENT TERRANCE L. TAYLOR
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

Sworn to before me this 20th day of May, 2024.

CHERYL A. EIFERT
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA